

MD. SAMIUZZAMAN KHAN (TAMIM)

Cybersecurity Executive | Technology & Security Leader | Cyber Risk | Cyber Resilience | AI-Driven Security Operations

Dhaka, Bangladesh | +880 1753 077713 | tamim.infosec@gmail.com

LinkedIn: <https://linkedin.com/in/tamim-infosec> | Web: <https://tamimkhan.info>

EXECUTIVE PROFILE

Cybersecurity executive with 20+ years of technology and security leadership across South Asia and Africa, progressing from enterprise architecture and identity security to building and leading large-scale Cyber Fusion Center operations and executive technology strategy. Proven record translating cyber risk into Board-level decisions, building high-performing security organizations, modernizing detection and response, and applying AI and automation to cyber defense.

AREAS OF EXPERTISE

Security Leadership: Cybersecurity Strategy & Roadmap, Security Governance & Operating Models, Cyber Risk Management, Security Program Management, Board & Executive Advisory, Security Budgeting & Investment Planning, Team Building & Mentoring, BCP/cyber resilience, and budget ownership

Security Operations: Cyber Fusion Center (CFC), 24x7 SOC, MDR, Detection Engineering, Threat Hunting, Threat Intelligence (CTI), Incident Response & Crisis Management, Digital Forensics, Malware Analysis, Red / Blue / Purple Team

Architecture & Technology: Zero Trust Architecture, SIEM, SOAR, EDR/XDR, NDR, UEBA, Cloud Security, Network & Perimeter Security, IAM / IGA / PAM, SSO, MFA, Identity Federation (SAML, OAuth 2.0, OIDC, Kerberos), Vulnerability & Exposure Management

Governance & Compliance: CIS Controls, MITRE ATT&CK, NIST CSF, ISO/IEC 27001 practices, PCI DSS, SOX, GDPR, Third-Party Risk, security policy/governance Business Continuity & Disaster Recovery, Security Awareness

Innovation: AI / Generative AI / Agentic AI for security operations, LLM & RAG architectures, LangChain / LangGraph, security automation, AI-driven SOC design, product and service line development

SIGNATURE ACHIEVEMENTS

- Architected and implemented an AI-augmented SOC using local LLMs, RAG and agentic workflows, reducing manual analyst triage effort by 70%.
- Built and scaled a Cyber Fusion Center serving 5+ enterprise customers, monitoring 100,000+ assets and processing 3TB+ of security telemetry per day.
- Reduced mean time to detect (MTTD) by 60% through XDR deployment, automated detection engineering and cross-domain correlation.
- Lifted audit compliance score from 78% to 96% and cut critical vulnerabilities by 45% via a risk-based exposure management program.
- Cut incident response and containment time by 40% by re-engineering SIEM/XDR detection logic, correlation rules and response playbooks.
- Reduced analyst workload by 60% through SOAR orchestration of repetitive triage and enrichment tasks.
- Compressed new client onboarding by 50% with a standardized asset discovery, log integration and threat modelling framework.
- Influenced multi-year cybersecurity investments exceeding USD 4 million across telecom, banking and enterprise customers.

PROFESSIONAL EXPERIENCE

SHORBORNO HOLDINGS LTD (<https://shorbornoholdings.com>) — Dhaka, Bangladesh Mar 2022 – Present
Managed Security Services Provider (MSSP), Cyber Fusion Center (the Next Gen-SOC)

Chief Technology Officer Jun 2026 – Present

- Own enterprise technology and cybersecurity strategy, architecture standards, technology risk management and the innovation roadmap, reporting to the Board of Directors.

- Architected the vision for an AI-driven Hyper SOC integrating AI-assisted detection, cross-domain correlation, proactive threat hunting, SOAR automation, threat intelligence and analyst augmentation.
- Own technology investment planning, cybersecurity portfolio prioritization and strategic vendor governance, aligning security expenditure with enterprise risk, customer requirements and business growth.
- Defined the enterprise-wide cyber defense strategy that reduced critical vulnerabilities by 45% and raised audit compliance score from 78% to 96%.
- Direct Managed Security Services for a national telecom operator, covering network, endpoint, application and cloud security with integrated monitoring, detection, incident response, vulnerability management, GRC, Red Team and AI/ML-enabled capabilities.
- Lead engineering, cloud, infrastructure, cybersecurity and product teams; own technology budgeting, portfolio management and vendor and system-integrator partnerships.
- Advance AI adoption in security operations — LLM and RAG architectures, Agentic AI, multi-model detection, LangChain/LangGraph, context engineering and controlled AI automation.
- Serve as executive cybersecurity advisor to customers, partners and the Board, influencing multi-year security investment decisions.
- Scaled cybersecurity and technology organization from 50 to 80 professionals across SOC, IR, Threat Intelligence, Threat Hunting, Detection Engineering, Red/Blue/Purple Teaming, IAM and GRC.

Head of Cyber Fusion Center

Jan 2025 – Dec 2025

- Led 24x7 Cyber Fusion Center operations across security monitoring, threat intelligence, threat hunting, incident response, risk management and security governance as a single operating framework.
- Built the CFC to support 5+ enterprise customers, 100,000+ monitored assets and 3TB+ of daily security telemetry.
- Drove the transition from traditional SOC to intelligence-led fusion operations; reduced MTTD by 60%.
- Established governance models, operating processes, KPIs, SLAs and executive reporting frameworks; improved compliance score from 78% to 96%.
- Directed Threat Intelligence, Threat Hunting and Red / Blue / Purple Team program, and led cyber crisis management and operational resilience.
- Integrated cyber risk management into enterprise governance through risk assessments, treatment planning and board-level risk reporting.
- Built and mentored a 50-member cybersecurity organization and its operational leadership layer.

Senior Security Architect, Cyber Fusion Center

Mar 2022 – Dec 2024

- Established the Cyber Fusion Center strategy, target operating model and reference architecture from greenfield.
- Architected integrated security ecosystems spanning SIEM, SOAR, EDR/XDR, NDR, UEBA, threat intelligence, cloud security, identity security and AI-driven automation.
- Built MDR services protecting 50,000+ endpoints across telecom, banking and enterprise clients.
- Developed 100+ custom detection use cases mapped to MITRE ATT&CK, improving coverage for ransomware, insider threat and APT activity.
- Engineered a hybrid log ingestion strategy across cloud, on-premises and OT/ICS environments, achieving full telemetry visibility across client estates.
- Directed cyber risk reduction through vulnerability management, exposure management and security hardening, with KPI-driven executive visibility.

TIGERIT BANGLADESH LTD (<https://www.tigerit.com>)— Dhaka, Bangladesh

Mar 2012 – Feb 2022

System integrator and software development company serving telecom, banking and government

Senior Solution Architect — Identity Governance & SOC

Jan 2021 – Feb 2022

- Provided executive-level leadership on enterprise and national-scale security architectures for telecom and government clients.
- Owned SOC, SIEM, SOAR, UEBA, NDR, EDR/XDR, IAM and PAM solution strategy, sizing and deployment across on-premises and cloud environments.
- Drove pre-sales, budgeting and security program roadmaps influencing multi-year cybersecurity investments.
- Engaged regulators, auditors and C-level stakeholders on compliance and risk alignment; supported MSS operations across Bangladesh and Sri Lanka.
- Delivered a Zero Trust model incorporating just-in-time privilege escalation, adaptive access controls and MFA; migrated legacy identity systems to cloud-based IAM, cutting authentication time by 80%.

Solution Architect — Identity Governance & SOC

Jan 2017 – Dec 2020

- Designed and implemented SOC platforms with centralized monitoring, threat hunting and incident response.
- Led enterprise IAM, access management, risk-based authentication and PAM (Delinea/Thycotic, Fudo PAM).
- Established compliance workflows and access governance frameworks that reduced policy violations by 40%.
- Conducted regional risk assessments and security testing across South Asia; delivered audit-ready identity governance, access certification and compliance reporting.

IAM Architect — Oracle IAM, PAM & Identity Governance

Jan 2014 – Dec 2016

- Designed and implemented SOA-based IAM solutions across Oracle Access Management, Oracle Directory Services, Oracle Identity Governance, Identity Analytics and audit platforms.
- Acted as security SME for IAM engagements and delivered organization-wide access certification and attestation programs enabling department-level governance and enterprise compliance assurance.

IAM Engineer — Oracle IAM

Mar 2012 – Dec 2013

- Deployed and integrated enterprise-scale IAM platforms in client production environments; designed identity workflows, approval chains and access governance, and supported solution scoping and risk-aware architectural tailoring.

EARLY CAREER

- **Senior Software Engineer, Cyber Jahan Ltd** (<https://cyberjahan.com>) — Dhaka, Bangladesh (Jan 2009 – Feb 2012). Led SDLC delivery, SOA web services, data modelling and high-availability environments (Oracle RAC, WebLogic, JBoss clusters).
- **Senior Database Administrator, Millicom (Tigo) SPRL** (<https://www.millicom.com>) — Kinshasa, DR Congo (Jan 2008 – Dec 2008). Deployed telecom VAS platforms on Oracle RAC and Data Guard; 24x7 support for business-critical billing and middleware services.
- **Database Administrator, DNS Software Ltd** (<https://www.dsl.com.bd>) — Dhaka, Bangladesh (Oct 2005 – Dec 2007). Designed telecom VAS database architectures and SMPP-based messaging services; Linux and Oracle administration for high-volume production platforms.

EDUCATION

Master of Information Security and Systems (MISS), CGPA 3.90:

Bangladesh University of Professionals (BUP) (<https://bup.edu.bd>), Dhaka — 2018–2019

Thesis: Self-Sovereign Identity Management Using Blockchain — decentralized digital identity to address identity theft, privacy and trust deficits in centralized identity systems.

Master of Business Administration (MBA), Management Information Systems, CGPA 3.78:

Ahsanullah University of Science and Technology (<https://www.aust.edu>), Dhaka — 2011–2012

BSc (Hons) Computer Science, First Class (75%):

National University, Bangladesh (<https://www.nu.ac.bd>) — 2001–2005

CERTIFICATIONS & PROFESSIONAL DEVELOPMENT

Certifications

- Certified SOC Analyst (CSA) — EC-Council
- Oracle Cloud Infrastructure 2023 Certified Architect Associate — Oracle University
- Oracle Identity Governance Suite 11g Certified Implementation Specialist — Oracle University
- Oracle Access Management Suite Plus 11g Certified Implementation Specialist — Oracle University
- Oracle Certified Professional (OCP), Oracle 10g Database Administrator — Oracle University

Executive & Technical Training

- Certified Chief Information Security Officer (C|CISO) — EC-Council
- OOP .NET Track (BASIS)

ADDITIONAL INFORMATION

Languages: Bangla (native), English (professional working proficiency), Hindi (limited working proficiency)

International Experience: 20+ years of technology and cybersecurity leadership across South Asia and Africa

Thought Leadership: Publishes on cybersecurity strategy, SOC architecture, cyber resilience and AI-driven security operations; selected articles and insights available on [LinkedIn](#)